DII COE Security
Software Requirements Specification (SRS)

Version 3.0

11 July 1997

Prepared for:
Defense Intelligence Agency

Prepared by:
The MITRE Corporation
1820 Dolley Madison Boulevard
McLean, VA 22102-3481

Comments on this document should be submitted to the following point of contact:

Mr. Mike Zajdek
Defense Intelligence Agency
Voice: (202) 231-2372
Fax: (202) 231-2400
E-Mail: curiosity@msn.com

or

Mr. Thomas A. Gregg
The MITRE Corporation
Voice: (703) 883-7032
Fax: (703) 883-1397
E-Mail: tgregg@mitre.org

TABLE OF CONTENTS

Section **Page**

SECTION 1

SCOPE

1.1 IDENTIFICATION

This document describes software requirements for the Defense Information Infrastructure (DII) Common Operating Environment (COE) security services.

1.2 SYSTEM OVERVIEW

This document specifies the software security requirements for the DII COE, but does not address the overall security requirements of systems built using the DII. The overall security requirements will be met by the COE security services software and other security disciplines (e.g., administrative, physical, personnel). Security services comprise one of six platform services defined in the *Architectural Design Document for the Defense Information Infrastructure Common Operating Environment* (Defense Information Systems Agency [DISA], 1996), which is intended to be compliant with the *Technical Architecture Framework for Information Management* (DISA, 1995), including Volume 6, the *Department of Defense Goal Security Architecture* (DISA, 1994). The security requirements specified in this document will be allocated across the COE platform services areas.

This Software Requirements Specification (SRS) identifies the requirements for the Security Services platform services area. The security services will function in a heterogeneous environment in the following six areas: accountability, availability, access control, confidentiality, integrity, and non-repudiation.

The DII COE will initially provide a foundation for systems that operate in a system high mode of operation. The objective mode of operation of the for many systems built on the DII COE is multilevel secure (MLS), which will demand additional security requirements above those required for system high operation. Looking to the future, however, this SRS does include some MLS mode requirements.

Service, agency, and system-unique security requirements are outside the scope of this document.

1.3 DOCUMENT OVERVIEW

This document outlines the software capabilities required to provide security services within the DII COE.

Section 2 lists documents referenced and documents that provide guidance applicable to this specification.

Section 3 details the security requirements for the security services, The security services include the following six areas: accountability, availability, access control, confidentiality, integrity, and non-repudiation.

Section 4 identifies the qualification provisions, including the methods used to ensure that the requirements in Section 3 have been met. Security testing, documentation, and assurance requirements are also presented in Section 4.

Section 5 addresses the traceability of each security requirement from a source security policy or requirements document. Section 5 also includes implementation priorities for each requirement.

Section 6 contains acronyms, abbreviations, and a glossary of terms and definitions needed to understand this document.

SECTION 2

DOCUMENTS

2.1 REFERENCED DOCUMENTS

In developing security requirements for this SRS, the following documents were referenced. Each document is to be given equal value and importance when developing/selecting security mechanisms to satisfy the security requirements. In the event of a conflict of interpretation, higher level DOD policy takes precedence over other instruments.

Department of Defense (DOD), *DOD Information Security Program*, Department of Defense Directive (DODD) 5200.1-R, 17 January 1997.

DOD, *Trusted Computer System Evaluation Criteria (TCSEC)*, DOD 5200.28-STD, December 1985.

DOD, *Security Requirements for Automated Information Systems (AIS)*, DODD 5200.28, 21 March 1988.

DOD, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, DODD 5230.11, 16 June 1992.

Defense Information Systems Agency (DISA), *Department of Defense Technical Architecture Framework for Information Management*, Version 3.0, 30 April 1996

DISA, *Architectural Design Document for the Defense Information Infrastructure Common Operating Environment*, DRAFT, January 1996.

Defense Intelligence Agency (DIA), *Security of Compartmented Computer Operations (U)*, DIA Manual 50-4, CONFIDENTIAL, October 1985.

DIA, *DOD Intelligence Information System (DODIIS) Security Architecture Guidance and Directions*, DIA, September 1994.

Director of Central Intelligence (DCI), *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)*, DCI Directive (DCID) 1/16, (SECRET), July 1988.

National Computer Security Center (NCSC), *Glossary of Computer Security Terms*, 21 October 1988.

National Institute of Standards and Technology (NIST), Federal Information Processing Standard 186, *date*

Rome Laboratory, *Segment Specification for the Client Server Environment - System Services*, Griffiss AFB, NY, July 1995.

497th Intelligence Group, *DODIIS Client Server Environment System Services Requirements*, Bolling AFB, Washington, DC, 8 February 1994.

2.2 GUIDANCE DOCUMENTS

DOD, *Department of Defense Joint Technical Architecture*, Version 1.0, 22 August 1996.

Department of Defense Computer Security Center, *Department of Defense Password Management Guide*, CSC-STD-003-85, 25 June 1985.

DISA, *GCCS Common Operating Environment Baseline*, LL-500-04-03, DISA, November 1994.

DISA, *GCCS Technical Security Functional Requirements Document*, DRAFT, 10 March 1995.

DISA, *Information Technology Standards Guidance (ITSG)*, Version 2.1, 30 September 1995.

DISA, *GCCS Automated Information System (AIS) Security Plan for Version 2.1*, 23 January 1996.

DISA, *GCCS Security Features Users Guide for Version 2.1*, 30 April 1996.

DISA, *GCCS Trusted Facility Manual for Version 2.1*, 21 June 1996.

DIA, *Security Requirements for System High Compartmented Mode Workstations*, DDS-2600-5502-87, DIA, November 1987.

DCI, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)*, DCID 1/16 Supplement, (SECRET), July 1988.

Executive Order 12958, *Classified National Security Information*, 17 April 1995.

Joint Chiefs of Staff, *Global Command and Control System (GCCS) Security Policy*, CJCSI 6731.01 30 April 1996.

Office of Management and Budget (OMB), Circular A-130, *Management of Federal Information Resources*, 8 February 1996.

SECTION 3

SECURITY REQUIREMENTS

The security requirements contained within this document reflect the DOD security policy and operational considerations, and assist systems in accomplishing their mission. The security services for the DII COE can be broadly categorized into the following six areas:

Accountability. The property that enables security-relevant activities on a system to be traced to individuals who may then be held responsible for their actions (NCSC, 1988).

Availability. The state when data is in the place needed by the user, at the time the user needs them, and in the form needed by the user (NCSC, 1988).

Access Control. The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

Confidentiality. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity. The property that information has not been altered or destroyed in an unauthorized manner.

Non-repudiation. The proof of delivery or origin of information transactions.

The level of assurance[1] necessary to determine if these services have been implemented correctly is a function of many factors. These factors are specific to the system that is being built with COE components and are difficult to pre-determine. However, the sensitivity of the data being processed on the system and the clearance levels of system users are two factors that must always be considered. Over time, selected COE components will be selected that have higher assurance. Assurance requirements are included in Sections 3.12, 3.15, and 3.16. Section 3.12 includes requirements that are related to the design and specification of security functionality, Section 3.15 includes requirements for configuration management, and Section 3.16 includes requirements related to security testing of that functionality.

[1] Assurance is a measure of confidence that the security features and architecture of the COE accurately mediate and enforce the security policy (NCSC, 1988).

3.1 REQUIRED STATES AND MODES

The security services requirements are applicable to all operational modes, including, but not limited to, training, emergency, backup, wartime, peacetime, idle, ready, and active. The security services software will remain the same during any operational mode.

3.2 SECURITY SERVICES CAPABILITY REQUIREMENTS

This section contains the requirements necessary to provide the Security Services for the DII COE. There is not a one-to-one mapping of the six broad areas of security services for the DII COE to the subsections within this section. The mapping is shown in Table 1. In addition assurance requirements are presented in Sections 3.2.15, 3.2.16, 3.16, and Section 4.

Table 1. Security Service Area Mapping to Subsection.

Security Service Area	**Subsection Title**	**Subsection Number**
Accountability	Identification and Authentication (I&A) Trusted Path Security Auditing	3.2.1 3.2.2 3.2.3
Availability	Availability	3.2.4
Access Control	Discretionary Access Control Mandatory Access Control Sensitivity Labels	3.2.5 3.2.6 3.2.7
Confidentiality	Markings Trusted Interfaces Object Reuse Data Confidentiality	3.2.8 3.2.9 3.2.10 3.2.11
Integrity	Data Integrity System Integrity System Architecture Trusted Facility Management	3.2.12 3.2.13 3.2.15 3.2.16
Non-repudiation	Non-repudiation	3.2.14

The security requirements in this section were derived from the guidelines set forth in the Department of Defense Directive 5200.28 (DOD, 1988), Department of Defense Directive

C-5200.1-R (DOD, 1982), DCID 1/16 (DCI, 1988), and DIA Manual 50-4 (DIA, 1985) and other system policy and design documents.

3.2.1 Identification and Authentication

3.2.1.1 The COE shall enforce individual accountability by providing the capability to uniquely identify each user to the system.

3.2.1.1.1 The COE shall require users to uniquely identify themselves before beginning to perform any actions that the system is expected to mediate.

3.2.1.1.2 The COE shall require users to login prior to assuming a trusted profile (e.g., system administrator, security officer, root user, super user).

3.2.1.2 Each user shall be uniquely identifiable (e.g., user name or userID) within an administrative domain.

3.2.1.2.1 The COE shall uniquely identify each user for an entire enterprise.

3.2.1.3 The COE shall provide the capability of associating the user's identity with all auditable actions taken by that individual.

3.2.1.4 The COE shall provide the following mechanism(s) to authenticate each user's identity.

3.2.1.4.1 The COE shall provide the capability to authentic each user's identity with a password. If passwords are used as the mechanism, they shall meet the following requirements:

3.2.1.4.1.1 The COE shall provide the capability for users, the security officer, or the system to generate passwords.

3.2.1.4.1.1.1 The COE shall provide a graphical user interface (GUI) for changing passwords.

3.2.1.4.1.1.2 The COE shall require a password be changed after the age of a password has exceeded a maximum of n days where n is configurable by a trusted user.

3.2.1.4.1.1.2.1 The default maximum days shall be 90.

3.2.1.4.1.1.3 The COE shall notify the user n days prior to password expiration where n is defined by a trusted user.

3.2.1.4.1.1.3.1 The COE shall default to notifying the user 5 days prior to password expiration.

3.2.1.4.1.1.4 The COE shall prohibit a password from being changed until the age of a password has exceeded a minimum of n days where n is defined by a trusted user.

3.2.1.4.1.1.4.1 The default minimum before a password can be changed shall be 5 days.

3.2.1.4.1.2 The COE shall permit a trusted user to override minimum password age limits when changing passwords.

3.2.1.4.1.3 When changing the password, the COE shall prohibit the reuse of the current password and n previous passwords used prior to the current password where n is defined by a trusted user.

3.2.1.4.1.3.1 The default number of previous passwords n shall be 2.

3.2.1.4.1.4 The COE shall only permit trusted users to change passwords other than their own.

3.2.1.4.1.5 The COE shall provide the capability to require users to change a password during the initial use of a password created by trusted users.

3.2.1.4.1.6 The COE shall provide the capability to prohibit the use of dictionary words or common passwords.

3.2.1.4.1.6.1 The COE shall provide the capability for a trusted user to include a list of dictionary words or common passwords that are prohibited.

3.2.1.4.1.7 The COE shall ensure that passwords feature specific characteristics configurable by a trusted user. The following characteristics shall be included:

3.2.1.4.1.7.1 Minimum password length

3.2.1.4.1.7.1.1 The default minimum password length shall be set to six characters.

3.2.1.4.1.7.2 Password character set (e.g., alphanumeric plus special American National Standard Code for Information Interchange [ASCII] characters).

3.2.1.4.1.7.3 Password includes at least one numeric, case change, or special character (e.g., 0-9, &, %).

3.2.1.4.1.8 The COE shall provide the capability to prohibit the following in passwords:

3.2.1.4.1.8.1 Strings of n repeating characters (e.g., ee) are prohibited, where n is configurable by a trusted user.

3.2.1.4.1.8.1.1 The COE shall default to prohibiting 2 repeating characters.

3.2.1.4.1.8.2 Use of user name within password is prohibited.

3.2.1.4.2 The COE shall provide the capability to authentic each user's identity with a hardware token (e.g., smart card, FORTEZZA card).

3.2.1.4.3 The COE shall provide the capability to authentic each user's identity with an X.509 version 3 certificate.

3.2.1.4.4 The COE shall provide the capability for strong user authentication (i.e., using cryptographically protected authentication or one-time passwords)

3.2.1.5 The COE shall prevent unauthorized access to authentication data.

3.2.1.5.1 The COE shall prevent unauthorized disclosure of passwords during transmission across a network.

3.2.1.5.2 The COE shall prevent unauthorized disclosure of passwords while stored.

3.2.1.6 The COE shall provide the capability to restrict consecutive login failures.

3.2.1.6.1 If the number of consecutive login failures reaches a threshold (0 through n) where n is configurable by a trusted user, the userID shall be locked and all further login attempts with that userID from within the administrative domain shall be prohibited.

3.2.1.6.2 The COE shall be configurable by a trusted user to provide the capability to set the default number of consecutive login failures.

3.2.1.6.2.1 The default number of consecutive login failures shall be three.

3.2.1.6.3 The COE shall provide the capability for a trusted user, and only a trusted user, to disable the consecutive login failure functionality.

3.2.1.6.4 When a userID is locked, the COE shall provide the capability to send a notification to a trusted user.

3.2.1.6.5 The COE shall provide the capability for a trusted user to restore locked userIDs.

3.2.1.6.6 The COE shall perform login failure lockout for all login points (e.g., console, remote login) in the administrative domain.

3.2.1.6.6.1 The COE shall perform login failure lockout for all login points (e.g., console, remote login) in the enterprise.

3.2.1.7 The COE shall provide a non-forgeable, non-replayable distributed authentication mechanism that supports both unilateral (client-to-server) or mutual (client-to-server and server-to-client) authentication.

3.2.1.8 The COE shall provide a single sign-on capability that permits access to resources (e.g., applications and information) in a distributed system for which the user is authorized without the user being required to reauthenticate at each host where the resources reside.

3.2.1.8.1 The COE shall provide the capability to restrict the time period for which a user may be permitted to use single sign-on to access resources to n minutes where n is configurable by a trusted user.

3.2.1.8.1.1 After n minutes the user shall be required to reauthenticate to access remote resources.

3.2.1.8.1.2 The default time period n for which a user may be permitted to use single sign-on shall be 480 minutes.

3.2.1.8.2 The COE shall support single sign-on using FORTEZZA as an authentication mechanism during the user's initial login.

3.2.1.8.3 The COE shall support single sign-on using X.509v3 certificates as an authentication mechanism during the user's initial login.

3.2.2 Trusted Path

3.2.2.1 The COE shall provide a trusted communications path between itself and the user for initial identification and authentication.

3.2.2.2 The COE shall ensure that communication via the trusted communications path is initiated exclusively by a user.

3.2.3 Security Audit

3.2.3.1 The COE shall provide the capability to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects.

3.2.3.1.1 The COE shall protect audit data so that access to it is limited to those who are authorized to view audit data.

3.2.3.1.2 The COE shall protect the audit processes and audit data from change or deletion by general users. At a minimum, the COE shall protect the following:

3.2.3.1.2.1 Audit mechanisms (e.g., executable files).
3.2.3.1.2.2 Configuration parameters (e.g., audit configuration files).
3.2.3.1.2.3 Capability to enable or disable audit processes.

3.2.3.1.3 The COE shall provide a mechanism that generates a notification when the audit data has reached a configurable threshold of n percent of available storage capacity.

3.2.3.1.3.1 The COE shall be configurable by a trusted user to provide a capability for recovery in the event that the threshold n percent of available storage capacity has been exceeded. At a minimum, the following capabilities shall be provided:

3.2.3.1.3.1.1 Halt the system
3.2.3.1.3.1.2 Overwrite previous audit data
3.2.3.1.3.1.3 Discontinue auditing

3.2.3.1.3.1.3.1 The default capability for recovery shall be to discontinue auditing.

3.2.3.1.3.2 The COE shall provide an interface for configuring which trusted user shall receive notifications when the audit data has reached the threshold n percent of available storage capacity.

3.2.3.1.3.3 The COE shall provide the capability for a trusted user to configure the threshold n percent of available storage capacity when a notification will be generated.

3.2.3.1.3.3.1 The default threshold n shall be 85 percent.

3.2.3.1.4 The COE shall provide a mechanism that generates a notification to a trusted user when the audit process(s) has failed.

3.2.3.1.4.1 The COE shall provide a capability for recovery in the event that the audit process(s) has failed. At a minimum, the following capabilities shall be provided:

3.2.3.1.4.1.1 Halt the system

3.2.3.1.4.1.2 Suspend user processing until audit process(s) are restarted

3.2.3.1.4.1.2.1 The default recovery capability shall be to suspend user processing until audit process(s) are restarted.

3.2.3.1.4.2 The COE shall provide an interface for configuring which trusted user shall receive notifications when the audit process(s) has failed.

3.2.3.1.5 The COE shall provide a capability to archive audit data.

3.2.3.1.5.1 The COE shall provide the capability to automatically archive audit data when the audit data reaches a configurable threshold of n percent of available storage capacity.

3.2.3.1.5.2 The COE shall provide the capability for a trusted user to configure the threshold of n percent upon which audit data will be automatically archived.

3.2.3.1.5.2.1 The default threshold shall be 70 percent.

3.2.3.2 The COE shall provide the capability to enable and disable auditable events.

3.2.3.3 The COE shall provide the capability to audit the following types of events:

3.2.3.3.1 Use of identification and authentication mechanisms

3.2.3.3.2 Introduction of objects into a user's address space (e.g., file open, program initiation)

3.2.3.3.3 Creation, modification, and deletion of objects

3.2.3.3.4 Actions taken by trusted users

3.2.3.3.5 Production of printed output

3.2.3.3.6 Override of human-readable output markings

3.2.3.3.7 Change in access control permissions

3.2.3.3.8 Export to external media

3.2.3.3.9 System startup

3.2.3.3.10 System shutdown

3.2.3.4 The COE shall provide the capability for a trusted user to define security-relevant events.

3.2.3.5 For each recorded event, at a minimum the COE audit record shall identify:

3.2.3.5.1 System date and time (to the nearest second) of the event

3.2.3.5.2 UserID

3.2.2.5.3 Type of event

3.2.3.5.4 Success or failure of the event

3.2.3.6 For identification and authentication events, the COE audit record shall identify the origin of the request (e.g., terminal ID, host IP address)

3.2.3.7 For events that introduce an object into a user's address space, and for object deletion events, the COE audit record shall identify the name of the object

3.2.3.7.1 In MLS systems, COE audit record shall identify the object's security level (e.g., sensitivity level and handling caveats).

3.2.3.8 The COE shall provide the capability to selectively audit the actions of any one or more users based on individual identity.

3.2.3.9 The COE shall provide the capability to correlate all system administrative and audit logs (e.g., database management system logs, operating system audit logs, and other system logs) within an administrative domain.

3.2.3.10 The COE shall provide the capability to receive application-level audit data (e.g., UNIX syslog, Windows NT event log).

3.2.3.11 The COE shall provide the capability to generate reports of audit data that has been collected.

3.2.3.11.1 The COE shall provide the capability to generate reports based on fields of event records or Boolean combinations of those fields.

3.2.3.11.2 The COE shall provide the capability to generate reports based on ranges of system date and time that audit records were collected.

3.2.4 Availability

3.2.4.1 The COE shall be capable of detecting the failure of a system service or resource.

3.2.4.1.1 The COE shall provide the capability to generate a notification to a trusted user upon failure of a COE system service.

3.2.4.1.1.1 The COE shall provide the capability to configure which trusted user shall receive notifications when a system service or resource fails.

3.2.4.1.1.1.1 The default trusted user who receives notifications when a system service or resource fails shall be the set of all trusted users defined for the COE.

3.2.4.1.2 The COE shall provide the following capabilities to notify a trusted user:

3.2.4.1.2.1 Electronic mail message to a trusted user account
3.2.4.1.2.2 Message to the console of a system where the trusted user is logged in
3.2.4.1.2.3 Message sent to a pager

3.2.4.1.3 Failure of a COE system service shall be logged in a system log file.

3.2.4.1.3.1 The type of failure and the time of the failure shall be logged.

3.2.4.1.4 Upon detection of a failed system service, the COE shall provide the capability to restart the service.

3.2.4.1.5 The COE shall provide a trusted user the capability to configure how the trusted user is notified when a system service or resource has failed.

3.2.4.1.5.1 The primary default capability for notifying the trusted user that a system service or resource has failed is a message to the console of a system where the trusted user is logged in.

3.2.4.1.5.2 The secondary default capability for notifying the trusted user that a system service or resource has failed is a message sent to a pager.

3.2.4.1.5.3 The tertiary default capability for notifying the trusted user that a system service or resource has failed is an electronic mail message to a trusted user account.

3.2.4.2 Upon recovery of a failed system resource, the COE shall verify that it returns in a secure state.

3.2.4.2.1 Upon recovery of a failed system resource, the COE shall provide the capability to determine if file systems are intact.

3.2.4.2.2 Upon recovery of a failed system resource, the COE shall provide the capability to determine if access control permissions are unchanged from the state prior to the failure.

3.2.4.2.3 Upon recovery of a failed system resource, the COE shall ensure that user privileges have not increased.

3.2.4.3 The COE shall provide the capability for a trusted user to selectively revoke a user’s access to services.

3.2.4.3.1 The COE shall provide the capability to kill or halt a user's process(es).

3.2.4.4 The COE shall provide the capability to perform system and database backups.

3.2.4.4.1 The COE shall provide the capability to scan for viruses during backup operations.

3.2.4.5 The COE shall provide the capability to recover from failures using system and database backups.

3.2.5 Discretionary Access Control (DAC)

3.2.5.1 The COE shall provide the capability to define access between named users and named objects (e.g., files, database elements, and programs).

3.2.5.2 The COE shall provide the capability to control access between named users and named objects (e.g., files, database elements, and programs).

3.2.5.3 The COE shall restrict access to objects based on the user's identity and on access rights (e.g., read, write, execute).

3.2.5.3.1 The COE shall provide the capability to restrict access to objects based on the user's profile (i.e., role-based access control).

3.2.5.3.2 The COE shall provide the capability to restrict access to objects based on the user's organization.

3.2.5.4 The COE shall provide the capability for users to specify and control sharing of objects by named users or defined sets of users (e.g., UNIX groups, access control lists), or by both.

3.2.5.5 The COE shall provide controls to limit the propagation of access rights.

3.2.5.6 The COE shall, either by explicit user action or by default, protect objects from unauthorized access.

3.2.5.7 The COE shall provide the capability to assign access rights to authorized users.

3.2.5.8 The COE shall permit a user to grant or revoke access to an object only if the user has control permission (e.g., file owner) for that object.

3.2.5.9 The COE shall provide a means to associate applications with a work environment (i.e., profiles) and allow users to specify the work environment (i.e., profile selection) during a session.

3.2.5.9.1 The COE shall permit a user to hold membership in multiple groups of users and have the access rights of those groups simultaneously.

3.2.5.10 DELETED. (Note: This requirement is covered by 3.2.15.2.)

3.2.5.11 The COE shall be capable of restricting access to input/output (I/O) devices (e.g., floppy disks and tape drives).

3.2.5.11.1 The COE shall provide a capability to specify which users may access which I/O devices.

3.2.5.12 The COE shall provide a deadman capability that is activated if user input devices have been idle for longer than a time period of zero to n minutes, where n is configurable by a trusted user.

3.2.5.12.1 When the deadman capability is activated, the COE shall perform one of the following actions where the selection of which action to perform shall be configurable by a trusted user.

3.2.5.12.1.1 The COE shall lock the user's terminal when the deadman is activated.

3.2.5.12.1.2 The COE shall logoff the user when the deadman is activated.

3.2.5.12.1.3 When the deadman is activated, the COE shall lock the user's terminal and after a time period of zero to n minutes, where n is configurable by a trusted user, the COE shall logoff the user.

3.2.5.12.2 The COE shall provide the capability to define a default time period for the deadman capability.

3.2.5.12.2.1 The configurable time period shall default to 5 minutes.

3.2.5.12.3 The COE shall provide the capability for a trusted user to disable the deadman capability.

3.2.5.12.4 Any user input device may be used to initiate actions to restore a locked terminal.

3.2.5.12.5 The specific input value (whether from keyboard, mouse, or other input device) used to restore a locked terminal shall be ignored except to initiate actions to unlock the terminal.

3.2.5.12.6 The COE shall require that users re-authenticate themselves to unlock a locked terminal.

3.2.5.12.7 The deadman capability shall be available for users to manually invoke.

3.2.5.12.8 The COE shall provide the capability for a trusted user to unlock a locked terminal irrespective of which user was logged in to that terminal.

3.2.5.13 The COE shall provide the capability to control access of mobile code (e.g., Java applets, ActiveX controls) to objects.

3.2.6 Mandatory Access Control[2]

3.2.6.1 The COE shall enforce a MAC policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the COE security services.

3.2.6.1.1 Subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical levels and categories, and the labels shall be used as the basis for mandatory access control decisions.

3.2.6.1.2 The COE shall support three or more hierarchical levels.

3.2.6.1.3 The COE shall support a minimum of 128 categories.

3.2.6.2 The COE shall mediate all accesses between subjects and objects providing that the following conditions have been met:

3.2.6.2.1 A subject can read an object only if the classification in the subject's security level is greater than or equal to the classification in the object's security level and the categories in the subject's security level include all the categories in the object's security level.

[2] MAC requirements are the B2 requirements from DOD 5200.28-STD. Not all COE components will need to implement MAC. MAC will be implemented incrementally as operational considerations require MLS mode and technology permits.

3.2.6.2.2 A subject can write an object only if the classification in the subject's security level is less than or equal to the classification in the object's security level and all the categories in the subject's security level are included in the categories of the object's security level.

3.2.6.3 The COE shall ensure that the security level and authorization of subjects created to act on behalf of the individual user are dominated by the clearance and authorization of that user prior to data access.

3.2.6.4 The COE shall provide the capability for authorized users to change the sensitivity label (e.g., upgrade or downgrade) of an object.

3.2.6.4.1 The COE shall provide the capability to audit any change of sensitivity label.

3.2.7 Sensitivity Labels[3]

3.2.7.1 The COE shall maintain sensitivity labels that are associated with each system resource (e.g., subject, storage object, read-only memory [ROM]) directly or indirectly accessible by subjects external to the COE.

3.2.7.1.1 The COE shall use sensitivity labels as the basis for mandatory access control decisions.

3.2.7.1.2 To import non-labeled data, the COE shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the COE.

3.2.7.2 The COE shall ensure that sensitivity labels accurately represent security levels of the specific subjects or objects with which they are associated.

3.2.7.2.1 When exported by the COE, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported (e.g., internal labels for an object would need to accurately map to Common Internet Protocol Security Option labels used during network transmissions).

3.2.7.3 The COE shall designate each communications channel and I/O device as either single-level or multilevel.

[3] Sensitivity labels are required for MLS mode.

3.2.7.3.1 Any change in the designation of single-level or multilevel shall be done manually by an authorized user.

3.2.7.3.2 The COE shall provide the capability to audit any change in single-level or multilevel designation.

3.2.7.3.3 When the COE exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported, shall reside on the same physical medium as the exported information, and shall be in the same form (i.e., machine-readable or human-readable form).

3.2.7.3.4 When the COE exports or imports an object over a multilevel communications channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

3.2.7.3.5 The COE shall include a mechanism by which the COE and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communications channels or I/O devices.

3.2.7.3.6 The COE shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session.

3.2.7.3.7 The COE shall provide the capability for a terminal user to query the COE for a display of the subject’s complete sensitivity label.

3.2.7.3.8 The COE shall assign minimum and maximum sensitivity levels to all attached physical devices.

3.2.8 Markings

3.2.8.1 The COE shall display a security warning prior to the login process that indicates the highest classification of information processed on the system.

3.2.8.2 The COE shall display a security warning during the login process that indicates misuse of the system is subject to applicable penalties.

3.2.8.2.1 This security warning shall state that the user accepts responsibility for his or her actions prior to being permitted to access information.

3.2.8.3 The COE shall provide the capability to surround each print job with banner pages reflecting the system high level of the system.

3.2.8.3.1 When operating in the multilevel mode, the COE shall mark the beginning and end of all printed output with human-readable sensitivity labels that properly represent the sensitivity of the output.

3.2.8.4 The COE shall provide the capability to label the top and bottom of each internal page of printed output with a sensitivity label representing the sensitivity of the output.

3.2.8.4.1 The internal page markings shall default to the system high label of the system.

3.2.8.4.2 When operating in the multilevel mode, markings on internal pages shall properly represent the sensitivity of the output.

3.2.8.5 The COE shall provide the user with print options to override the printing of the banner pages and internal page markings.

3.2.8.5.1 The COE shall provide the capability to audit any override of the printing of banner pages and internal page markings.

3.2.8.6 The COE shall provide the following forms of markings for labeling printed output:

3.2.8.6.1 Highest classification of information processed on the system

3.2.8.6.2 Markings that represent the actual security level (classification and compartments) of the information being printed

3.2.8.6.3 Applicable markings (codewords, dissemination and control markings and handling caveats)

3.2.8.7 The COE shall provide a GUI-based interface from which the user selects the destination printer, number of copies, and sensitivity label from the set of authorized markings.

3.2.9 Trusted Interfaces

3.2.9.1 The COE shall provide a capability to review and release information to systems of disparate security levels.

3.2.9.2 The COE shall provide the capability to audit the release of information to systems of disparate security levels.

3.2.10 Object Reuse

3.2.10.1 The COE shall ensure that no information, including encrypted representations of information, produced by a prior subject's actions is made available to any subject that obtains access to an object that has been released back to the COE.

3.2.10.2 The COE shall ensure that all authorizations to information contained within a storage object have been revoked prior to initial assignment, allocation, or reallocation to a subject from the COE's pool of unused storage objects.

3.2.11 Data Confidentiality

3.2.11.1 The COE shall provide an interface to cryptographic application programming interfaces for use by applications to selectively encrypt and decrypt data and files.

3.2.11.2 The COE shall provide the capability for end-to-end encryption services for user sessions.

3.2.11.2.1 The COE shall provide end-to-end encryption using a unique private key for each user.

3.2.11.2.2 The COE shall protect the confidentiality and integrity of user private keys.

3.2.11.2.3 The COE shall provide the capability for a user to transport his or her private key from one user platform to another user platform.

3.2.12 Data Integrity

3.2.12.1 The COE shall provide the capability to detect unauthorized modification or destruction of data during storage (e.g., using digital signatures and hash codes on files).

3.2.12.1.1 The COE shall provide the capability to audit unauthorized modification or destruction of data during storage.

3.2.12.2 The COE shall provide the capability to detect modification or destruction of data that occur while in transit over communications channels (e.g., using cryptographic checksums or digital signatures).

3.2.13 System Integrity

3.2.13.1 The COE shall provide the capability to validate the correct operation of the hardware, software, and firmware elements of the COE security services.

3.2.13.2 The COE shall provide the capability to automatically validate the correct operation of the hardware and firmware elements of the COE security services during recovery from failure.

3.2.13.3 The COE shall be configured such that a password must be entered to boot to a single-user state.

3.2.13.4 The COE shall provide the capability to detect and eradicate malicious code (e.g., viruses).

3.2.13.4.1 The COE shall provide the capability to for a user to initiate the scan hard drives and removable media for malicious code and alert the user and a trusted user if such code is detected.

3.2.13.4.2 The COE shall provide the capability to automatically scan hard drives and removable media for malicious code.

3.2.13.4.3 The COE shall provide the capability to alert the user and trusted user of the detection of malicious code by the following techniques:

3.2.13.4.3.1 Visible message on the workstation screen
3.2.13.4.3.2 Audible alarm

3.2.13.5 The COE shall provide the capability to eradicate the malicious code or delete the file containing the code.

3.2.14 Non-repudiation

3.2.14.1 The COE shall provide the capability for the recipient of an information transaction to determine proof of the origin and originator of the data (e.g., using digital signatures).

3.2.14.2 The COE shall provide the capability for the sender of an information transaction to determine proof of delivery (e.g., using digital signatures).

3.2.15 System Architecture

3.2.15.1 The COE security services shall maintain a domain for their own execution that protects them from external interference or tampering (e.g., by modification of their code or data structures).

3.2.15.2 The COE shall isolate resources to be protected so that they are subject to the access control and auditing requirements.

3.2.15.3 The COE shall implement the principle of least privilege such that each subject is granted the most restrictive set of privileges needed for the performance of authorized tasks.

3.2.16 Trusted Facility Management

3.2.16.1 The COE shall support trusted facility management via segregation of authorized roles.

3.2.16.1.1 At a minimum the COE shall provide security officer, systems administrator, and user roles.

3.2.16.1.2 The COE shall provide the capability to create trusted roles.

3.2.16.1.3 The COE shall provide the capability to assign security-relevant functions to a trusted role.

3.2.16.1.4 The COE shall provide the capability to modify trusted roles.

3.2.16.1.4.1 The COE shall provide the capability to add security-relevant functions to a trusted role.

3.2.16.1.4.2 The COE shall provide the capability to delete security-relevant functions from a trusted role.

3.2.16.1.4.3 The COE shall restrict to a trusted role the capability to modify the security-relevant functions of a trusted role.

3.2.16.1.5 The COE shall provide the capability to delete trusted roles.

3.2.16.1.6 The COE shall prohibit security-relevant functions from being assigned to non-trusted roles.

3.2.16.2 The COE shall provide the capability to manage accounts for authorized users.

3.2.16.2.1 The COE shall provide the capability to create accounts for authorized users.

3.2.16.2.2 The COE shall provide the capability to modify accounts for authorized users.

3.2.16.2.3 The COE shall provide the capability to delete accounts for authorized users.

3.2.16.3 The COE shall provide the capability to manage profiles for groups of users with common access rights.

3.2.16.3.1 The COE shall provide the capability to create profiles or groups of users with common access rights.

3.2.16.3.2 The COE shall provide the capability to modify the access rights of profiles or groups of users.

3.2.16.3.3 The COE shall provide the capability to delete profiles or groups of users.

3.2.16.4 The COE shall provide the capability to purge data from fixed and removable storage media or assignable storage devices.

3.2.16.5 The COE shall provide a standard set of security support tools to determine the security posture of COE systems.

3.2.16.5.1 The COE shall provide the capability to validate that passwords have met the requirements for password characteristics specified in Paragraph 3.2.1.4.1.7.

3.2.16.5.2 The COE shall provide the capability to determine if changes have been made to designated systems and applications files, (e.g., password or rc.* files).

3.2.16.5.3 The COE shall provide the capability for a trusted user to monitor and analyze the configuration of a host.

3.2.16.5.3.1 The COE shall provide the capability verify the configuration of a system to ensure that the security policy has been implemented (i.e., check for current security patches, check that unneeded network services are turned off).

3.2.16.6 The COE shall provide the capability to manage sensitivity labels and handling caveats used in marking printed output.

3.2.16.6.1 The COE shall provide the capability to enable or disable marking printed output with sensitivity labels and handling caveats.

3.2.16.6.2 The COE shall provide a GUI-based capability for creating a set of authorized sensitivity labels and handling caveat values for use in marking printed output.

3.2.16.6.3 The COE shall provide a GUI-based capability for modifying the set of authorized sensitivity labels and handling caveat values that are used in marking printed output.

3.2.16.6.4 The COE shall provide a GUI-based capability for deleting of the set of authorized sensitivity label and handling caveat values that are used in marking printed output.

3.2.16.7 The COE shall provide a GUI-based capability to manage the configuration of the audit system.

3.2.17 World Wide Web and Network News Servers

3.2.17.1 COE Web Server(s) shall provide userID/password-based identification and authentication.

3.2.17.2 COE Web Server(s) shall provide the capability to create, modify, and delete user groups.

3.2.17.3 COE Web Server(s) shall provide the capability to create, modify, and delete access control lists (ACLs) that authorize list members to access the following types of objects:

3.2.17.3.1 Document trees
3.2.17.3.2 Directories
3.2.17.3.3 Files

3.2.17.3.4 Uniform Resource Locator
3.2.17.3.5 Document
3.2.17.3.6 Subsets of a Document

3.2.17.4 COE Web Servers(s) shall provide the capability to modify an ACL without restarting the Web Server.

3.2.17.5 COE Web Server(s) shall provide the capability to log the user, pathname, and time of access of all file accesses.

3.2.17.6 COE Web Server(s) shall provide the capability to automatically archive log files.

3.2.17.7 COE Web Server(s) shall provide the capability to securely remotely configure and maintain the server.

3.2.17.8 COE Web Server(s) shall provide security services using the Secure Sockets Layers protocol.

3.2.17.8.1 COE Web Server(s) shall support SSL version 2.0.

3.2.17.8.2 COE Web Server(s) shall support SSL version 3.0.

3.2.17.8.3 COE Web Server(s) shall support the SSL protocol for the following network services:

3.2.17.8.3.1 World Wide Web (i.e., HyperText Transfer Protocol [HTTP])
3.2.17.8 3.2 Network News Transfer Protocol (NNTP)
3.2.17.8.3.3 Lightweight Directory Access Protocol (LDAP)

3.2.17.9 COE Web Server(s) shall provide the capability to prohibit connections by Internet domain name.

3.2.17.10 COE Web Server(s) shall provide the capability to prohibit connections by Internet Protocol (IP) address.

3.2.17.11 COE Network News Server(s) shall provide the capability to securely remotely configure and maintain the server.

3.2.17.12 COE Network News Server(s) shall provide the capability to replicate news articles.

3.2.17.13 COE Network News Server(s) shall provide the capability to create, modify, and delete ACLs that authorize list members to access news groups.

3.2.17.14 COE Network News Server(s) shall provide the capability to control access to news groups based on Internet domain name.

3.2.17.15 COE Network News Server(s) shall provide the capability to control access to news groups based on IP address.

3.2.17.16 COE Network News Server(s) shall provide the capability to log errors.

3.2.18 Database Access

3.2.18.1 The COE shall provide the capability to monitor user access to databases for the following security relevant events:

3.2.18.1.1 Attempts to change access control permissions
3.2.18.1.2 Attempts to create, copy, sanitize, purge, or execute databases

3.2.18.2 The COE shall provide the capability to create, modify, and delete database access control permissions (i.e., grant permissions) at the following levels:

3.2.18.2.1 Table
3.2.18.2.2 View
3.2.18.2.3 Row or record
3.2.18.2.4 Field or element

3.2.18.3 The COE shall provide the capability to define access control permissions for the following:

3.2.18.3.1 User(s)
3.2.18.3.2 Profile
3.2.18.3.3 Workstation.

3.2.18.4 The COE shall provide the capability to assign access control permissions to objects for which a user does not already possess permission to trusted user(s) and only to trusted user(s).

3.2.18.5 The COE shall provide the capability to label data base information at the following levels of abstraction:

3.2.18.5.1 Database
3.2.18.5.2 Data row or record
3.2.18.5.3 Data field or element

3.2.19 Digital Signatures

3.2.19.1 The COE shall provide the capability to create and verify digital signatures.

3.2.19.2 The digital signatures support by COE shall meet the following standards:

3.2.19.2.1 The Digital Signature Standard (DSS) as specified in FIPS Publication 186

3.2.19.2.2 RSA as specified in PKCS#1

3.2.20 Interface to Public Key Infrastructure

3.2.20.1 The COE shall provide the capability to request creation of X.509 and PKCS #7 and #10 certificates.

3.2.20.2 The COE shall provide the capability to receive and store X.509 and PKCS #7 and #10 certificates.

3.2.20.3 The COE shall provide the capability to request certificate revocation lists (CRL).

3.2.20.4 The COE shall provide the capability to request third-party X.509 and PKCS #7 and #10 certificates.

3.2.20.5 The COE shall provide the capability to validate third-party X.509 and PKCS #7 and #10 certificates. Validation of third-party certificates shall include the following:

3.2.20.5.1 Verifying the certificate of the certifying authority of the certificate

3.2.20.5.2 Verifying the certificate chain (i.e., checking the validity dates and signature of the certificate issuer for the original certificate, the issuer's certificate, etc., until a trusted authority is reached)

3.2.20.5.3 Verifying that the certificate is not on the CRL

3.2.20.5.4 Verifying that the validity period of the certificate has not expired

3.2.20.5.5 Verifying that the certificate is being used for its intended purpose.

3.3 SECURITY SERVICES EXTERNAL INTERFACE REQUIREMENTS

The security services interface with other COE components shall be through a software application program interface (API) among the application, mission, and support programs and all security services capabilities.

3.3.1 Interface Identification and Diagrams

To be specified (TBS)

3.3.2 Project-Unique Identifier Of Interface (TBS)

3.3.2.1 The Security Services shall have a set of standard APIs to the commercial off-the-shelf (COTS) security administration tools, in order that mission applications and other COE software can access security services functionality using a non-vendor-specific interface.

3.3.2.2 The security services shall have an interface to the Data Access System of the COE for file and database access control and audit information requests.

3.3.2.3 The security services shall have an interface to the Alert Services module of the COE to report selected security services related failures.

3.3.2.4 The security services shall have an interface to the Executive Manager module of the COE for process management, session management, and desktop management.

3.3.2.5 The security services shall have an interface to the System Administration software components to be used within the COE.

3.3.2.6 The security services shall provide an interface to the Office Automation functional area for office automation software packages (e.g., word processing, email, spreadsheet) to be used within the COE.

3.3.2.7 The security services shall provide an interface to the Message Processing functional area for message receiving, logging, routing, storage, retrieval, parsing, generation, coordination, transmission and delivery.

3.3.2.8 The security services shall provide an interface to the On-Line Support functional area for On-Line Support services such as Context Sensitive Help, On-Line Documentation, Job Planning, and Computer-Based Training.

3.3.2.9 The security services shall provide an interface to the Network Services functional area for communications security within the COE.

The COE security services will interface with other functional areas that require or provide a security-relevant audit event.

3.4 SECURITY SERVICES INTERNAL INTERFACE REQUIREMENTS

The design of the security services internal interface has not been determined at this time. These requirements will be developed during the software design process.

3.5 SECURITY SERVICES INTERNAL DATA ELEMENT REQUIREMENTS

TBS

3.6 ADAPTATION REQUIREMENTS

None

3.7 SAFETY REQUIREMENTS

None

3.8 SECURITY AND PRIVACY REQUIREMENTS

Systems built on the COE (e.g., GCCS, DODIIS, Global Combat Service and Support, Electronic Commerce/Electronic Data Interchange) must satisfy policy or requirements appropriate to their respective domains. The COE security services can be used to meet most of these requirements. The COE security requirements in Section 3.2 were derived from the guidelines set forth in the Department of Defense Directive 5200.28 (DOD, 1988), Department of Defense Directive C-5200.1-R (DOD, 1997), DCID 1/16 (DCI, 1988), and DIA Manual 50-4 (DIA, 1985) and other system policy and design documents.

3.9 ENVIRONMENT REQUIREMENTS

The security services must be portable and shall be implemented on all hardware and software platforms of the DII COE.

3.10 COMPUTER RESOURCE REQUIREMENTS

The computer resource requirements have not been determined at this time but will be compatible with the hardware and software platforms of the DII COE.

3.11 SOFTWARE QUALITY FACTORS

The design of the security services will be in line with software quality factors identified in the contract or derived from a higher level specification. Examples of software quality factors include reliability, maintainability, availability, flexibility, portability, reusability, testability, and usability (the ability to be easily learned and used).

3.12 DESIGN AND IMPLEMENTATION CONSTRAINTS

3.12.1 Assurance

For the multilevel mode of operation, the COE components that provide multilevel functionality shall meet the following life-cycle assurance design and verification requirements:

3.12.1.1 A formal model of the security policy support by the COE component shall be maintained over the life cycle of the component that is proven consistent with its axioms.

3.12.1.2 A Descriptive Top-Level Specification (DTLS) of the component shall be maintained that completely and accurately describes the component in terms of exceptions, error messages, and effects.

3.12.1.2.1 The DTLS shall be shown to be an accurate description of the COE component interface.

3.12.2 Implementation Dependencies

Dependencies on other software:

- Relational Data Base Management System (RDBMS): Sybase 11.0, Oracle 7.1.2, and Informix 7.1

- Operating system versions: HP-UX 9.07, HP-UX 10.1, Solaris 2.4, Solaris 2.5.1, Windows NT 3.51, Windows NT 4.0

Security services functions must operate in a distributed computing environment and/or client server environment.

3.13 PERSONNEL-RELATED REQUIREMENTS

None

3.14 TRAINING-RELATED REQUIREMENTS

None

3.15 LOGISTICS-RELATED REQUIREMENTS

For the multilevel mode of operations, the COE components providing security functionality shall meet the following configuration management requirements.

- During development and maintenance of the COE component, a configuration management system shall be in place that maintains control of changes to the DTLS, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation.

- The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the COE component.

- Tools shall be provided for generation of a new version of the COE component from source code.

- Also available shall be tools for comparing a newly generated version with the previous COE component version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the component.

Within the DISA Engineering Office or other appropriate office, a capability shall be provided to disseminate appropriate information on identified security vulnerabilities and countermeasures related to the COE users.

3.16 OTHER REQUIREMENTS

The following documentation shall be developed for the user and system administrators to describe the COE security features and how to use and administer them:

- The COE *Security Features User's Guide* (SFUG), which is a single summary, chapter, or manual in user documentation, shall describe the security mechanisms provided by the COE, how they interact with one another, and guidelines on their use by general, unprivileged users.

    - The COE SFUG shall provide instructions for COE users to perform I&A-related functions.

    - The COE SFUG shall provide instructions for COE users to perform DAC-related functions on COE.

- The COE *Trusted Facility Manual* (TFM), which is a manual addressed to the COE system administrator, shall present cautions about functions and privileges that should be controlled in order to manage COE securely.

    - The COE TFM shall provide instructions for system administrators to configure the I&A mechanisms of COE; and to define, modify, and delete COE user account information.

    - The COE TFM shall provide instructions for the security officer to configure and maintain the audit mechanisms of COE (including the events to be audited, the audit trail retention period, and the audit review frequency).

    - The COE TFM shall specify procedures for maintaining and reviewing COE audit files.

    - The COE TFM shall describe the detailed audit record structure for each type of audit event.

    - The COE TFM shall provide instructions for system administrators to properly configure and maintain the DAC mechanisms of the COE.

- COE certification and accreditation shall be supported by three test documents:
  - Certification Test Plan
  - Certification Test Procedures
  - Certification Test Report
- Documentation shall be available that describes how the COE safeguards satisfy COE security requirements.
- Documentation shall be available that describes how COE security-enforcing functions interface with one another and with other COE components.

3.17 PACKAGING REQUIREMENTS

None

3.18 PRECEDENCE AND CRITICALITY OF REQUIREMENTS

The order of precedence or criticality indicating the relative importance of the requirements in this specification is related to the security mode of operation. Those requirements related to a system high mode of operation are higher in criticality than those related to a multilevel mode of operation (e.g., mandatory access control, sensitivity labels).

SECTION 4

QUALIFICATION PROVISIONS

This section identifies the qualification provisions including the methods used to ensure that the requirements in Section 3 have been met.

4.1 QUALIFICATION METHODS

Qualification methods, such as demonstrations, tests, analysis, inspection and any other special tools, techniques, and procedures to ensure that the requirement has been met have not been determined at this time.

4.2 SECURITY TESTING

Security testing of the COE shall be accomplished in accordance with Department of Defense Directive 5200.28 (DOD, 1988).

Security testing for a system high mode of operation shall include the following:

- The security mechanisms of COE components shall be tested and found to work as claimed in the system documentation.

- Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the COE.

- Testing shall also include a search for obvious flaws that would allow violation of resource isolation or permit unauthorized access to the audit or authentication data.

In addition to that for system high, security testing for a MLS environment shall include the following:

- A team of individuals who thoroughly understand the specific implementation of the COE security services shall subject its design documentation, source code (if available), and object code to thorough analysis and testing. This team's objectives are to:

    - Uncover all design and implementation flaws that would permit a subject external to the COE security services to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the COE.

  - Assure that no subject (without authorization to do so) is able to cause the COE security services to enter a state such that they are unable to respond to communications initiated by other users.

- The COE security services shall be found to be relatively resistant to penetration.

- All discovered flaws shall be corrected and the COE security services retested to demonstrate that they have been eliminated and that new flaws have not been introduced.

SECTION 5

REQUIREMENTS TRACEABILITY

This section addresses the traceability of each security requirement to a corresponding source document or the service or agency that requested the requirement. The requirements trace also includes an indication as to whether or not the requirement has been met, not met, and if not, which version of the COE the capability will be implemented.

5.1 CAPABILITY REQUIREMENTS MATRIX

This matrix has yet to be developed. The matrix will be based on the traceability matrix distributed to the Security Services Working Group and DISA in March 97. In the final draft of the SRS, this matrix will be provided separately for security reasons.

SECTION 6

NOTES

This section contains acronyms, abbreviations and a list of terms and definitions needed to understand this document.

6.1 ACRONYMS AND ABBREVIATIONS

ACL	access control list
AIS	automated information system
ASCII	American national Standard Code for Information Interchange
API	application program interface
CRL	certificate revocation list
COE	Common Operating Environment
COTS	commercial off-the-shelf
CSE-SS	Client Server Environment System Services
DAC	Discretionary Access Control
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense Directive
DODIIS	Department of Defense Intelligence Information System
DTLS	Descriptive Top-Level Specification
E.O.	Executive Order
GCCS	Global Command and Control System
GUI	graphical user interface
I&A	identification and authentication
ID	identifier
I/O	input/output
IP	Internet Protocol
ITSG	Information Technology Standards Guidance

HP-UX	Hewlett-Packard UNIX Operating System
MAC	Mandatory Access Control
MLS	multilevel secure
NCSC	National Computer Security Center
OMB	Office of Management and Budget
RDBMS	relational database management system
ROM	read-only memory
SAGD	Security Architecture and Guidance Document
SFUG	Security Features User’s Guide
SRS	Software Requirements Specification
SSL	Secure Sockets Layer
STD	Standard
TAFIM	Technical Architecture Framework for Information Management
TBS	to be specified
TCSEC	Trusted Computer System Evaluation Criteria
TFM	Trusted Facility Manual
UserID	user identifier
X	X Window System

6.2 GLOSSARY

The following list identifies the terms that are used in this document along with their associated meanings.

administrative domain

The set of computing platforms and their associated resources (e.g., users, profiles, segments) that are under the administrative control of a single entity.

access

A specific type of interaction between a subject and an object resulting in the flow of information from one to the other.

access control

The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

access rights

The set of types of interaction between subjects and an object resulting in the flow of information from one to the other (e.g., owner-read and execute; group-read; others-none).

accountability

The property that enables activities on a system to be traced to individuals who may be held responsible for their actions.

audit trail

A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a transaction from its inception to final results.

assurance

A measure of confidence that the security features and architecture of the COE accurately mediate and enforce the security policy.

availability

The state when data is in the place needed by the user, at the time the user needs them, and in the form needed by the user

classification

A term that represents the hierarchical portion of the security level.

confidentiality

The concept of protecting data from unauthorized disclosure.

deadman function

A capability that locks or makes inoperable the user’s terminal or workstation if the user does not use the input devices (e.g., keyboard, mouse, trackball) for a configurable time period.

discretionary access control

A means of restricting access to objects based upon the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

DoD Trusted Computer System Evaluation Criteria (TCSEC)

A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is Government Standard DoD 5200.28-STD and is frequently referred to as “The Criteria” or “The Orange Book.”

identification and authentication

The combination of a process that enables recognition of an entity by a system, generally by the use of unique machine-readable names (identification) and the verification of the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system (authentication).

integrity

The degree of protection for data from intentional or unintentional alteration or misuse.

least privilege

The principle that requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

manage

The act of configuring, administering, operating, and maintaining the COE security requirements.

markings

Markings are human-readable labels presented on computer screens, printed on paper or affixed to removable media that describe the sensitivity of the information presented as to its classification, caveats, and handling restrictions or provide warnings to users in compliance with federal laws and regulations.

mechanism

A capability which must be properly managed in order to enforce the COE security requirements.

message data

TBS.

mode of operation

A description of the conditions under which an AIS functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users.

multilevel secure

A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and need-to-know, but prevents users from obtaining access to information for which they lack authorization.

multilevel secure mode of operation

A mode of operation in which all of the following statements are satisfied about each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:

- Some do not have valid personnel clearance for all the information processed in the AIS.

- All have the proper clearance and have the appropriate formal access approval for that information to which he/she is to have access.

- All have a valid need-to-know for that information to which they are to have access.

non-repudiation.

The proof of delivery or origin of information transactions.

object

A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

password

(1) A protected/private character string used to authenticate an identity. (2) A discretionary access control mechanism that represents the access control matrix by row by attaching passwords to protected objects.

purge

The removal of sensitive data from an Automated Information System (AIS), AIS storage device, or peripheral device with storage capacity, at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. After a purge, the medium can be declassified by observing the review procedures of the respective agency.

read access

A fundamental operation that results only in the flow of information from an object to a subject.

roles

The assignment of a user to a specific functionality within a system or application.

sensitivity labels

A piece of information that represents the security level of an object. Sensitivity labels are used by the COE Security Services as the basis for mandatory access control decisions.

security level

The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

security measures

Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications.

security policy

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

security resources

The software, hardware, and firmware components of a computer system responsible for implementing security measures.

security-relevant event

Any event that attempts to change the security state of the system (e.g., change discretionary access controls, change the security level of the subject, change user password). Also, any event that attempts to violate the security policy of the system (e.g., too many attempts to log in, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file).

security requirements

The types and level of protection necessary for equipment, data, information, applications, and facilities to meet a security policy.

secure state

A condition in which no subject can access any object in an unauthorized manner.

subject

An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

system high mode of operation

A mode of operation in which all of the following statements are satisfied about each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts and has all of the following:

- A valid personnel clearance for all information on the AIS.

- Formal access approval for, and has signed nondisclosure agreements for all the information to which he/she is to have access.

- A valid need-to-know for that information to which he/she is to have access.

system resources

Those entities that belong to and are controlled by the system.

trusted profile

The applications and resources that a trusted user is authorized to access in performance of their duties.

trusted users

Those users that have administrative responsibilities for the system that require the use of privileged commands to perform their duties (e.g., security officer, systems administrator).

trusted path

A mechanism by which a person at a terminal or workstation can communicate directly with the security services of the COE. This mechanism can only be activated by the person or the security services and cannot be imitated by untrusted software.

user

Any person who interacts directly with a computer system.

write

A fundamental operation that results only in the flow of information from a subject to an object.

write access

Permission to write to an object.